TECHNICAL COMMUNICATIONS CORPORATION
Communicate in Confidence
100 DOMINO DRIVE • CONCORD, MA 01742-2892 • U.S.A. • 508-287-5100 • FAX: 508-371-1280

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., N.W., Room 2705
Washington, D.C. 20230

12 Feb 1997

Re: Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List

Dear Ms. Crowe,

As regards the interim rule which provides for the transfer as noted above, there are a couple of issues which could perhaps be clarified and would assist in the transition.

The first is the definition of products which will remain on the U.S. Munitions List, and continue to be controlled by the Department of State, Office of Defense Trade Controls. According to the interim rule, "Encryption Items" subject to the EAR do not include encryption items specifically designed, developed, configured, adapted, or modified for military applications. There may be some confusion around the definition of military equipment. Is military equipment strictly defined as those items which contain U.S. military encryption? Technical Communication Corporation (TCC), among its products, manufactures and exports equipment for military use. Two products in particular are the DSP9000 Series of Radio Ciphering Systems and the DSD72A-SP Military High Speed Encryption Product. These products contain proprietary encryption, not U.S. military encryption. Yet, as the attached product brochures illustrate, they are designed for military use. The interim rule, as written, is not clear regarding such products.

A second concern is the anticipated level of administrative and paperwork burden required under this change. When applying through the State Department there were essentially two methods for obtaining export approval. The predominate method was the Warehouse and Distribution Arrangement. This provided for the shipment of most of TCC's products to most countries in the world. The required administrative tasks were the maintenance of a list of products shipped and their dollar value, forwarding of Shipper's Export Declarations to the Department of State, and the submittal of semiannual reports. Products or countries not covered by the Arrangement were processed with individual permanent license applications. These individual license applications for State were less detailed than those for Commerce and were less stringent in their requirement

TECHNICAL COMMUNICATIONS CORPORATION
Communicate in Confidence
100 DOMINO DRIVE • CONCORD, MA 01742-2892 • U.S.A

for support information. State required a copy of the customer purchase order or contract, a clear definition of the end use and user, technical specifications (as provided in product brochures), and the list of freight forwarders used by the company. Commerce requires somewhat more information on the application and can require an additional form for multiple end-users and another form for multiple products shipped under one order. Commerce may also require import/end-user certificates, technical specifications, letters of explanation, and perhaps other documentation. If the intent of the change to Commerce was to reduce the administrative burden when applying for export licenses, the objective may have been missed. Perhaps some of the procedures previously followed by State could be adopted by Commerce to help streamline the process a bit without compromising the intent or integrity of the system.

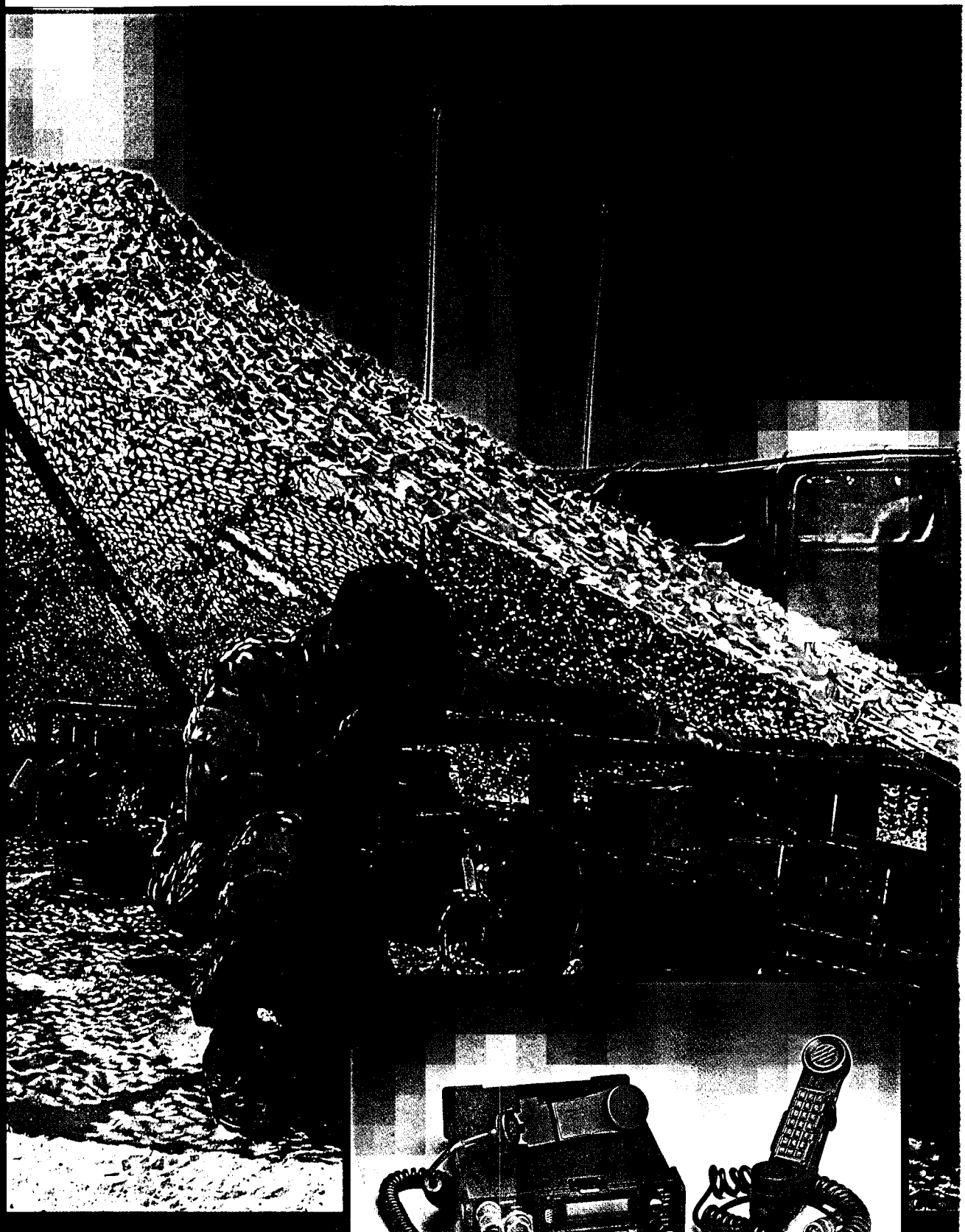
It is understandable how, in implementing such a major shift in procedure, a number of questions and issues would arise both for the export license applicants as well as though responsible for processing the applications. I look forward to continuing dialogue regarding the above issues as well as the resolution of other issues which may have been raised.

Sincerely,

Walter Kopek
Director of Operations

DSP 9000

Radio
Ciphering
System

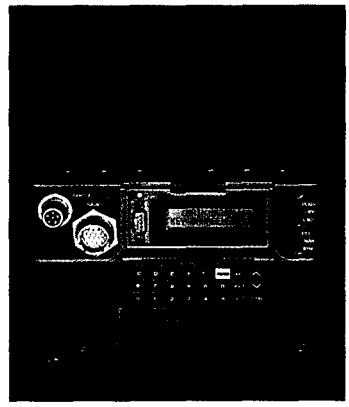


TCC

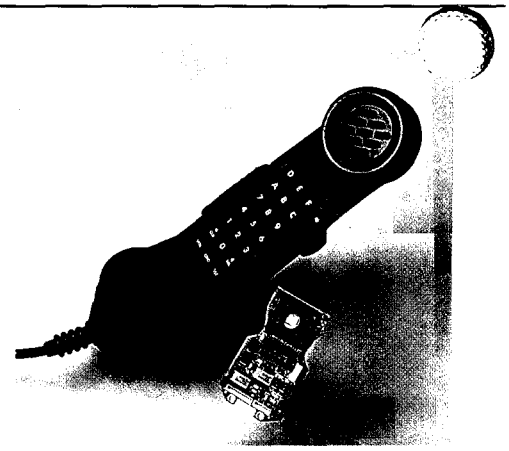
DSP 9000

Military Radio Ciphering System

The DSP 9000 is a family of Military Ciphering Systems that provide long-term, strategic security for communications transmitted over narrowband channels. The DSP 9000 is available in base station, manpack, handset, and implant board configurations. A programmable interface and MIL-SPEC design make the DSP 9000 capable of securing virtually any HF, VHF or UHF application.



TCC's DSP 9000 base station for fixed military installations.



The DSP 9000 handset replaces the radio handset for manpack applications.

Secure Applications

- HF-SSB, VHF, and UHF radio
- Radio teletype
- Standard dial-up telephones
- Low speed data
- Facsimile (Group I and Group II)
- Tactical switchboards and field telephones

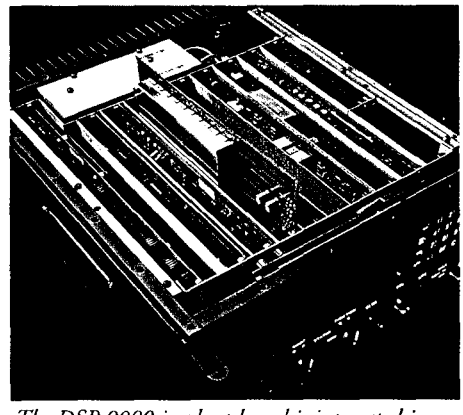
Advanced Technology

The DSP 9000 utilizes leading-edge technology throughout its design. A powerful Digital Signal Processor supplies tremendous computing power that is used to ensure exceptional recovered voice quality and cryptographic security. All audio input/output parameters are software controlled. This allows a single DSP 9000 to be quickly installed on a variety of radios without modifying the hardware.

Exclusive features such as half and full duplex versions, dual synchronization, automatic voice/data encryption selection, and storage of a large number of keys also clearly separate the DSP 9000 from its competitors. Additionally, the DSP 9000 is compatible with TCC's CSD 3324E secure telephone to enable "office-to-field" communication.

Features

- Strategic cryptographic security
- Exceptional recovered voice quality
- Half and full duplex models
- Menu driven, programmable interface and configuration
- Designed and tested to MIL-SPEC standards
- Full remote control capability for vehicles, ships and aircraft
- Select Call Mode for private conversations
- PTT and Manual synchronization
- Sync Coast feature
- Automated key management
- Fixed, mobile and manpack configurations



The DSP 9000 implant board is integrated in the radio system to secure radio communications.

Key Management and Cipher Technique

TCC's Enhanced Domain Transform encryption technique begins by using a "toll quality" voice digitizer operating at 64 Kbps. The digitized audio is then pseudo randomly transformed from frequency into time and time into frequency using TCC's "Enhanced Domain Transform" technique. This transform combined with a TCC proprietary compression technique eliminates virtually any residual intelligibility.

The domain transform is controlled by a highly non-linear digital key generator. This crypto algorithm can be modified by the customer using TCC's Crypto Management System. One of the selected encryption keys stored in the DSP 9000 and a randomly generated Initialization Vector (IV) provide a new keystream for each synchronization.

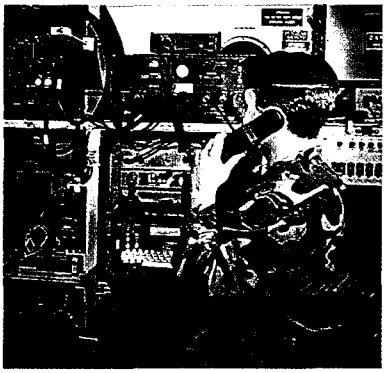
TCC's completely automatic 'hands off' key management approach is ideal for military applications. All key management parameters can be selected and controlled by a COMSEC security officer, thereby eliminating potential operator errors or compromise. The transmitting

unit selects the appropriate key by means of a real time clock at a time interval set by the security officer. Automatic downline key indexing insures that the receiving unit always selects the proper key for decryption.

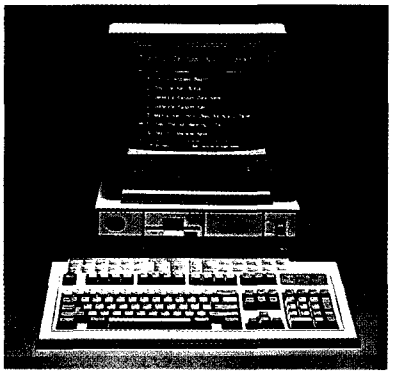
Handset and Implant Models

Advanced DSP technology and the latest miniaturization techniques have allowed the high-level security and voice processing of the DSP 9000 base station to be reduced in size to fit in a handset configuration, and as a board integrated into a radio.

It is no longer necessary for field soldiers to carry a separate crypto unit. The DSP 9000 HS replaces the existing radio handset, thereby adding less than one pound to the weight of the manpack radio. Prior to a mission, a security officer loads the DSP 9000 HS with 200 keys and radio interface settings using TCC's SmartModule™. Once loaded, the radio operator need only select cipher or plain mode. With the addition of the HS model, the DSP 9000 family now provides a complete, integrated security solution for air, ground and sea operations.



Fixed DSP 9000 base station installation in a communications shelter.



The crypto management system facilitates key generation, loading, and distribution.

The DSP 9000 Implant Board is an embedded, modular encryption option board designed for easy integration into HF, VHF and UHF radios. Radios using the DSP 9000 Implant Board will interoperate with radios secured with a full-size DSP 9000 unit or a DSP 9000 HS handset unit. New radios can be phased in, and radios from different manufacturers can communicate securely.

Quality

TCC is dedicated to quality products and services. TCC is ISO 9001 certified. ISO 9001, granted to TCC by TUV, is the most stringent standard available for total quality systems in design/development, production, installation and servicing.

Technical Specifications — DSP 9000 Family

CIPHERING TECHNIQUE	TCC proprietary Enhanced Domain Transform (EDT), controlled by a non-linear Key Generator
CRYPTO KEY VARIABLES	System key: 8.39×10^{79} Network key: 6.55×10^{4} Local key: 7.2×10^{16} Total keys: 4.0×10^{101}
SYNCHRONIZATION	Inband digitally controlled FSK sync burst (74 bits)
FREQUENCY CONTROL	High-stability crystal oscillator
FREQUENCY OFFSET	±120 Hz maximum for HF-SSB
AUDIO INTERFACE	'Soft' Selectable Interface Characteristics
AUDIO BANDWIDTH	Voice Mode: 200 Hz to 2800 Hz Data Mode: 200 Hz to 3000 Hz
REQUIRED CHANNEL BANDWIDTH	500 Hz to 2400 Hz Minimum
DIAGNOSTICS	BITE run at power on and on demand from keypad
ENVIRONMENTAL	Humidity: 120 hours, 95% non-condensing MIL-STD-810C, Method 507
EMI	MIL-STD-461B, Class A3
MTBF	Exceeds 10,000 hours per MIL-HDBK-217F & MIL-STD-756

Technical Specifications continued on the next page.

DSP 9000

Technical Specifications *continued*

DSP 9000 Base Station

KEY MANAGEMENT	Key Storage: 800 Local Keys stored in two key-banks containing 400 keys Key Loading: SmartModule™ or KFD-800 keyfill devices, or keypad entry
OPERATION	Half duplex and full duplex models
SIZE AND WEIGHT	Height: 2.25" (5.7 cm) Width: 8.25" (21 cm) Depth: 11.0" (28 cm) Weight: 5.7 lbs (2.6kg) half duplex 6.8 lbs (3.1kg) full duplex
POWER	DC Voltage: +9 to +32 VDC AC Voltage: 115/230 VAC, 50/60 Hz Current: 1 watt (90mA@12VDC)
AUDIO INTERFACE	H-189/HC-250 handset 4 wire/600 ohm MIC/Speaker Telephone direct wired
PUSH TO TALK SIGNAL	Contact closure to ground or to positive supply (+32 V max.)
DIAGNOSTICS	Full range of BITE including: CPU, RAM, ROM, DSP, analog test, audio loop, keypad, keyfail, key storage and display.
ENVIRONMENTAL	Temperature: Operating: -20° C to +70° C Storage: -40° C to +85° C Vibration: 1.5G peak, 55-220 Hz MIL-STD-810C, Method 514 Shock: 40G's @ 11ms MIL-STD-810C, Method 516
OPTIONS AND ACCESSORIES	■ TCC secure phone ■ KFD-800 keyfill device ■ SmartModule keyfill device ■ Remote control head ■ 19 inch rack mount ■ Shock mount assembly ■ Automatic Test Equipment ■ Crypto Management System

DSP 9000 Handset

KEY MANAGEMENT	Key Storage: 200 Local Keys stored in two keybanks containing 100 keys Key Loading: SmartModule™ keyfill device, or keypad entry
OPERATION	Half duplex
SIZE AND WEIGHT	Height: 9" (23 cm) Width: 2" (5.1 cm) Depth: 4" (10.2 cm) Weight: 2.0 lbs (.9kg)
POWER REQUIREMENTS	Externally supplied, 9 - 18 VDC 1 watt (90 mA @ 12 VDC)
AUDIO INTERFACE	6-pin MIL-C-55116 connector Aux connectors with DC power Others available on request
PUSH TO TALK SIGNAL	Contact closure to ground
ENVIRONMENTAL Temperature:	Operating: -20° C to +60° C Storage: - 40° C to +85° C
Waterproof:	Submersible to 1 meter
Vibration:	1 Grms, 5-200 Hz random curve, MIL-STD-810D, Method 514.3
Shock:	100 G's at 11 ms MIL-STD-810D, Method 516.3

DSP 9000 Implant Board

KEY MANAGEMENT	Key Storage: 200 Local Keys stored in two key-banks of 100 keys Key Loading: SmartModule™ or keypad entry
SYNCHRONIZATION	Inband digitally controlled FSK sync burst (74 bits)
OPERATION	Half-duplex (Push-to-Talk)
POWER	DC Voltage: 5V DC Input Current: 220mA (typical)
SIZE AND WEIGHT	Length: 9.75" (248 mm) Width: 3.78" (96 mm) Height: 0.7" (18 mm) component side 0.15" (4 mm) solder side Weight: 6 oz.
ENVIRONMENTAL Temperature:	Operating: -20° C to +70° C Storage: -40 ° C to + 70 ° C
EMI	4-layer board with separate ground and power planes RFI filtering on I/O signals Metal EMI shield over components

Printed in the U.S.A.

DCN 96 -1042

Technical Communications Corporation
100 Domino Drive
Concord, MA 01742-2892, U.S.A.
Tel: (508) 287 - 5100
Fax: (508) 371 - 1280
E-Mail: info@tccsecure.com
Web Site: http://www.tccsecure.com

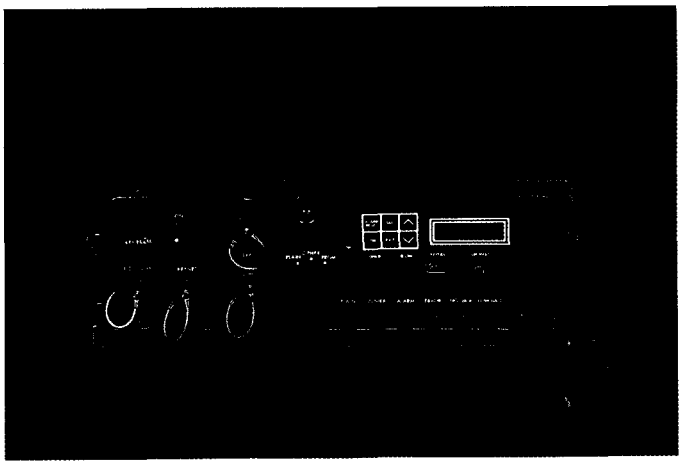
DSD 72A-SP

Military
High Speed
Encryption

TCC

DSD 72A-SP

Military High Speed Encryption System



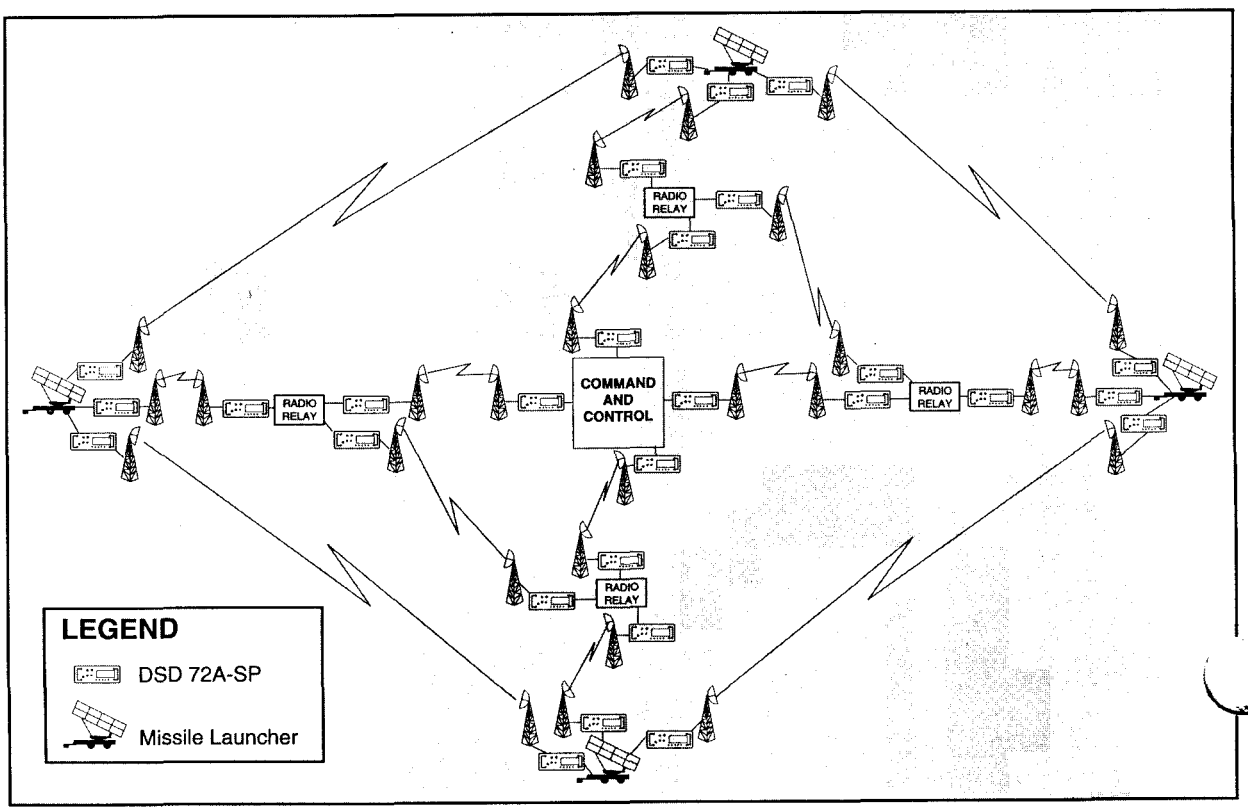
The DSD 72A-SP Encryption System provides strategic security for high data rate signals in demanding environments. Critical applications such as missile firing commands, emergency military telephone networks, and command and control networks are protected today by the DSD 72A-SP.

Maximum cryptologic security for military and top-level government applications is achieved with TCC's SNARK™ key generator and automated key management. Two crypto synchronization methods, long cycle and cipher feedback, are built into the system and allow it to stay on-line in a variety of error and jamming environments.

An anti-missile and anti-aircraft missile system, shown below, is a typical application for the DSD 72A-SP. Important acquisition and targeting information along with the actual firing commands are routed from a central site to the missile launchers. This information is encrypted by the DSD 72A-SP for both confidentiality and to prevent spoofing. Spoofing is when an unauthorized party sends false firing signals to the launchers to have them fire at the wrong time or at the wrong target. All of the encryption units are controlled by TCC's Centralized Crypto Management System (CMS) located at the Command & Control Headquarters.

Applications

- Missile Systems
- Radio Relay Networks
- Microwave Systems
- C^3I Networks
- Troposcatter Systems



Proven Design

The DSD 72A-SP has been designed, tested and field proven to operate in demanding environments. Over 2,000 units are on-line today in all regions of the world protecting highly classified information. The systems are tested under the severe conditions specified in Mil Spec 810D for temperature, humidity, vibration, rain, and other elements.

Quality is designed and manufactured into all of TCC's systems. The factory is MIL-Q-9858A certified, and the company is committed to ISO 9001 quality certification in 1995.

Features

- Strategic cryptologic security
- Automated key management
- Multiple interface and synchronization options
- Mil Spec, field proven design
- System tested and approved

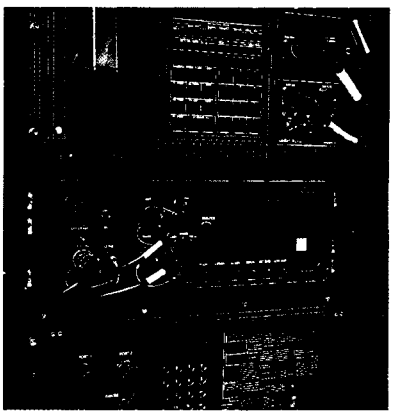
Key Management

Automated and secure key management throughout the key life cycle is provided by TCC's DSD 72A-SP and Crypto Management System (CMS). The DSD 72A-SP stores 800 keys, a much greater number than any other system, to minimize the need to load new keys.

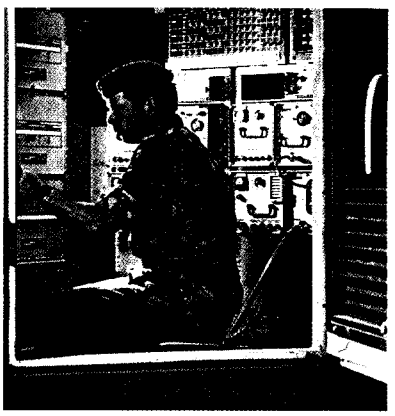
Truly random keys are generated and allocated by the CMS. TCC's SmartModule™ and KFD 800C, two high capacity and secure key transport devices, are used to deliver and load keys into the encryption units. The keys are encrypted for distribution so a loss of a key transport device does not jeopardize the security of the network.

Once the full set of 800 keys are loaded into the unit, key management is automatic. Keys can automatically be changed on a timed basis. Even with daily changing keys, new keys need only be loaded once every two years. Downline indexing keeps a communicating pair of DSD 72A-SP units on the same key. No sensitive keying information is sent over the air, only the key index numbers are sent.

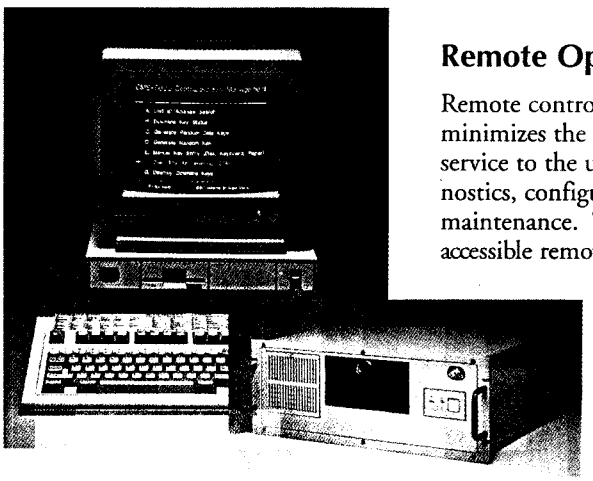
All keys are stored in a battery backed RAM capable of retaining the keys for five years without power. Tamper resistant packaging causes keys to be erased if a unit is opened. Keys may also be destroyed quickly and simply from the front panel to protect their secrecy in case of imminent overrun.



DSD 72A-SP with NFT-Ericsson radio and switch.



Typical DSD 72A-SP environment – shelter with CMC radio/mux equipment.



IBM based Crypto Management System available in commercial and ruggedized models.

Remote Operations

Remote control of encryption minimizes the need to send field service to the unit for ordinary diagnostics, configuration or preventive maintenance. This information is accessible remotely in both centralized and decentralized networks.

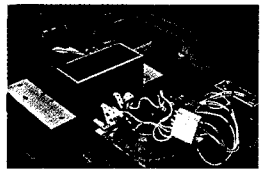
In centralized networks, a CMS with Command Link™ connection to each DSD 72A-SP can do most everything that can be done at the front panel of each unit in the network. Diagnostics, access to error and alarm logs, configuration, key allocation and usage and other functions are available and programmable at the CMS system.

In decentralized networks, on the other hand, DSD 72A-SP units form communicating pairs with each pair having a designated Master unit. The Master unit is placed at the more accessible site and has the ability to check remote unit status, run remote diagnostics and access error and alarm codes.

DSD 72A-SP

Technical Specifications

CRYPTOLOGY	Key Generators: SNARK™, PK^{2}M or MKG non-linear key generators Modes of Operation: Cipher Feedback and Long Cycle Mode both with automatic synchronization
KEY MANAGEMENT (SNARK)	Crypto Key Variables: 120-bit Local Key 8-bit Network Key 128-bit MKEK (Optional) Key Storage: 800 Local Keys stored in two keybanks Key Loading: SmartModule™ encrypted key transport and KFD 800C electronic keyfill device
DATA RATE	Full Duplex at 64 Kbps to 8 Mbps
REMOTE OPERATION	Diagnostics from remote DSD 72A-SP CMS centralized control of key management, configuration and diagnostics
INTERFACE OPTIONS	CCITT G.703/CEPT E1 CCITT G.703/CEPT E2 North American T1 Eurocom D/1 ATACS Tritac V.35/RS-422 Other interfaces upon request
POWER	DC: 24V or 48V nominal, ±20% AC: 85V to 264V, 47Hz to 440Hz Power Consumption: 20W maximum



ENVIRONMENTAL per MIL STD 810D	Operating Temperature: -20° C to +70° C Storage Temperature: -40° C to +85° C Humidity: 95% for 240 hours Method 507.2, Procedure III Rain: Method 506.2, Procedure I Transit Drop: Method 516 Shock: Method 516.3, Procedure I Vibration: Method 514.3, Procedure I Altitude: Method 500.2, Procedure II EMI: MIL STD 461A, CS02, CS06, RS03 MTBF: Ground Fixed 12,000 hrs. Ground Mobile 8,000 hrs.
SIZE AND WEIGHT	35.6 D x 43.2 W x 15.3 H cm 14 L x 17 W x 6 H inches 11.4 kg (25 lbs)
DIAGNOSTICS (BITE)	On-line tests: No data, keyfail, CPU, ROM integrity and key table integrity Off line tests: CPU, RAM, ROM, LED, LCD, keypad, self-loop and Command Link™
ACCESSORIES	■ Crypto Management System (CMS) ■ SmartModule ■ KFD 800C ■ Installation Kits ■ 19" Rack Mount ■ Shock Mount ■ Model 70 Test Fixture

DCN 94-1069

Technical Communications Corporation

100 Domino Drive
Concord, MA 01742
Tel: (508) 287 - 5100
Fax: (508) 371 - 1280
E-mail: marktng@teccom.com